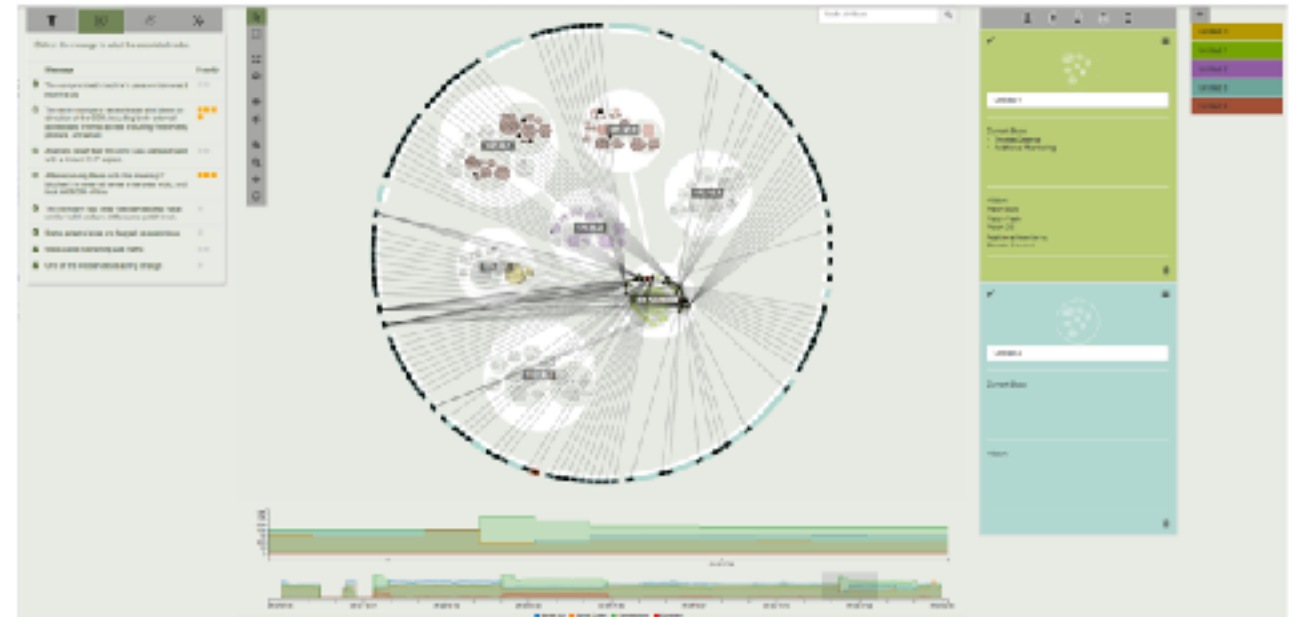
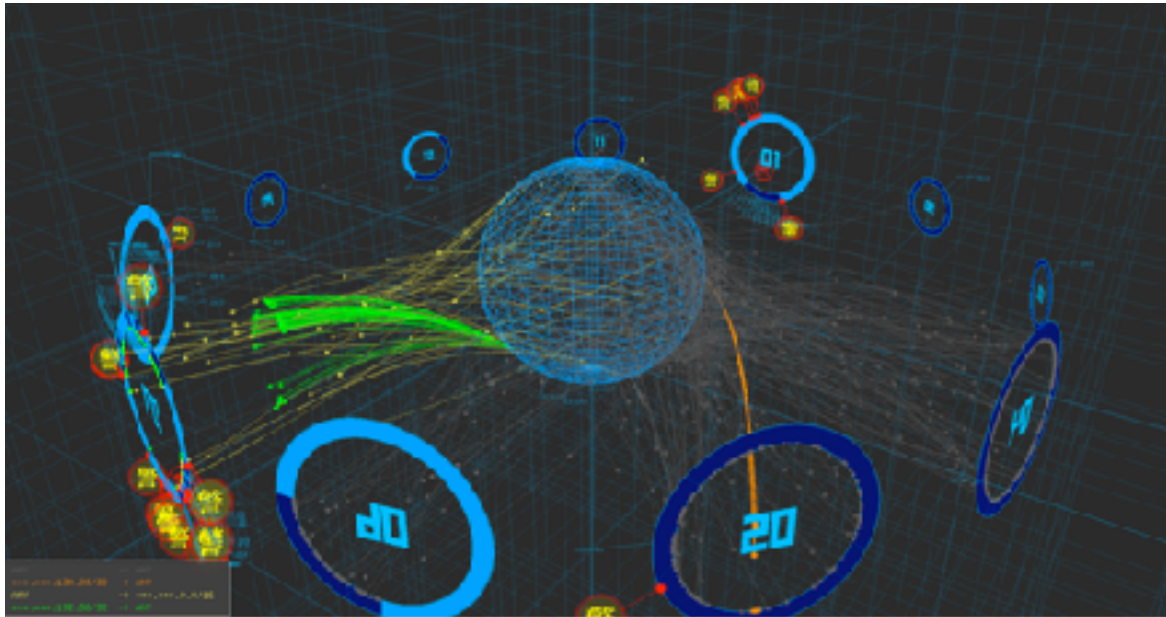


# 混合网络中的异常检测

# 背景介绍

- 异常检测

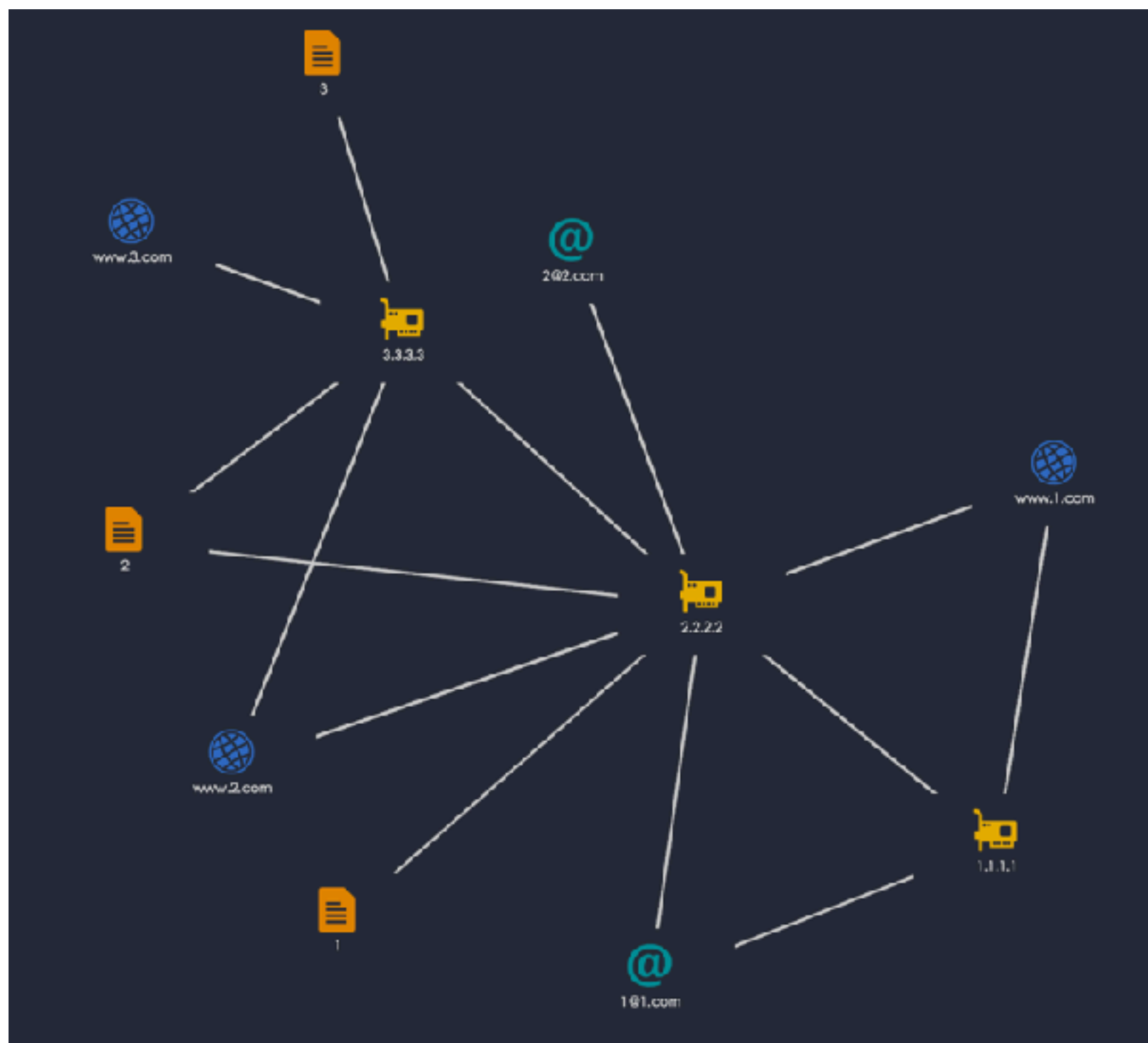


# 背景介绍

- 数据特点

序号	源ip	目标ip	发送人	接收人	url	样本文件
1	1.1.1.1	2.2.2.2	<u>sender@qq.c</u> <u>om</u>	<u>receiver@qq.c</u> <u>om</u>	<u>www.qq.com</u>	ad

# 背景介绍



# 问题描述：

## 混合网络中的异常检测

- 异常

1. IP间的异常流量

2. 异常数量的样本文件

3. 异常频繁的下载/上传操作

4. 异常频繁的发件/收件事件

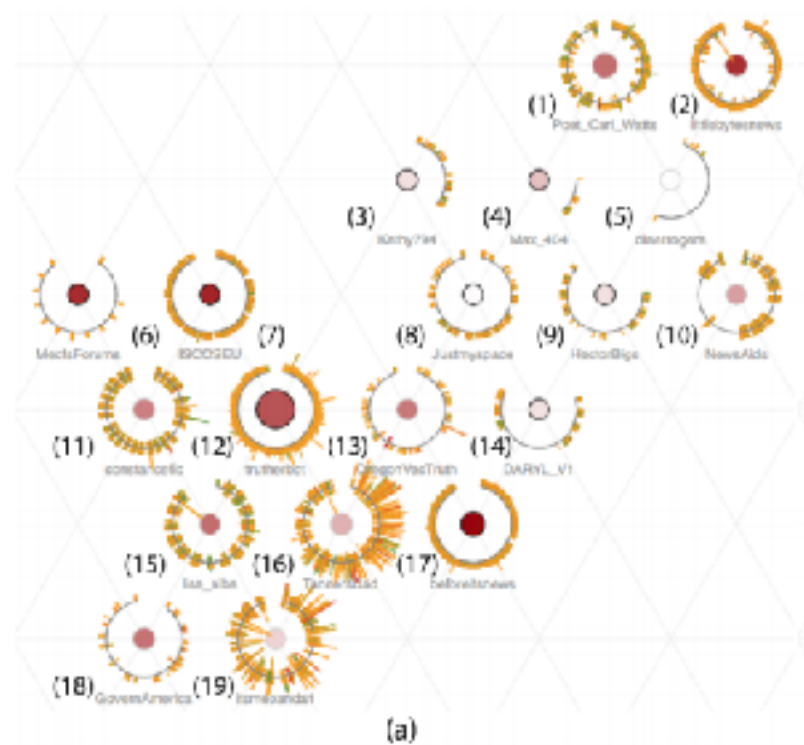
5. 具有异常流量的url

6. 异常主题的样本文件

7. 异常格式的样本文件

# 实现期望： 异常计算

- 对混合网络中的各类型节点分别建模计算异常值



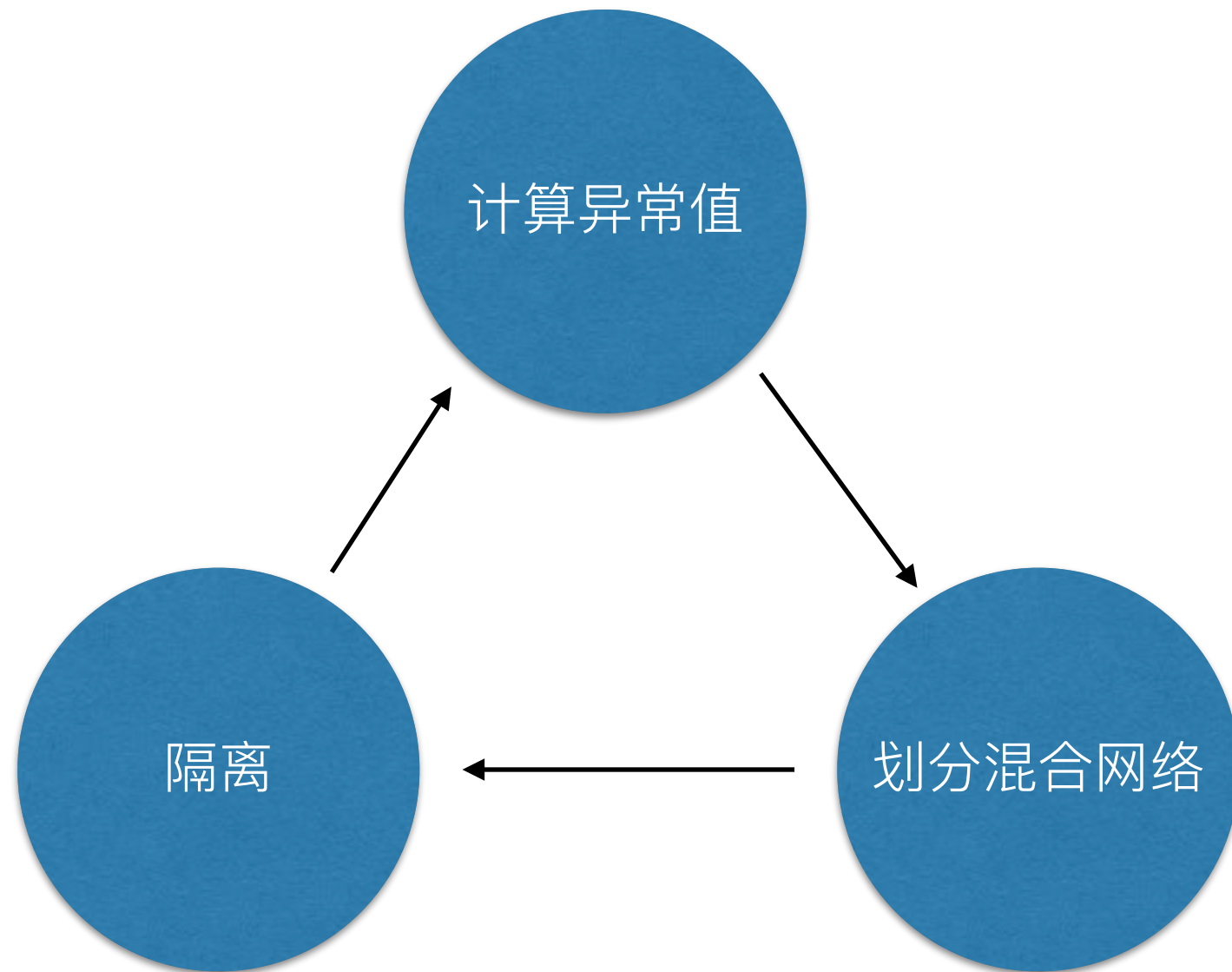
局部离群值模型 (TLOF) :

在某个用户的K个最近邻空间计算该  
用户的离群值

# 实现期望： 异常评估

- 根据网络中节点异常值的分布，对混合网络进行划分
- 根据划分结果和分析结果，隔离部分划分区域
- 对未被隔离区域异常评估
- 对被隔离区域异常评估

# 实现期望： 异常评估





# 主要贡献

- 对混合网络的可视分析
- 对网络异常行为的量化分析和评估

# 局限性和挑战

- 对异常值计算的模型选择
- 对动态混合网络的异常检测